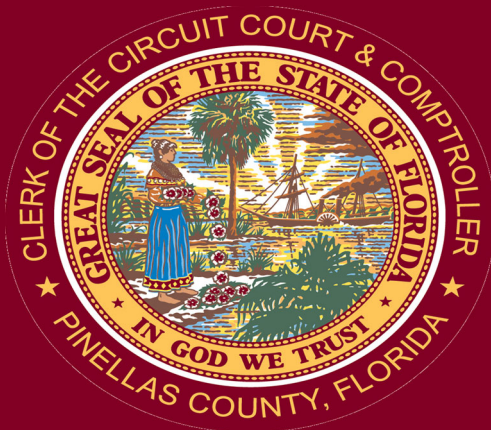




DIVISION OF INSPECTOR GENERAL
Ken Burke, CPA
Clerk of the Circuit Court and Comptroller
Pinellas County, Florida



AUDIT OF CLERK'S OFFICE DRIVER LICENSE TRANSCRIPT DATA EXCHANGE

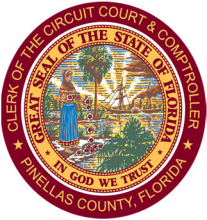


Melissa Dondero, CPA, CIA, CIG, CIGA, CIGI, CITP, CRMA, CFS, CECFE, CGI
Inspector General/Chief Audit Executive

Audit Team

Robert Poynter, CIGA, CIGI, CISA, CCA, CECFE, CFS - Assistant Inspector General
Jason Stanley, CFE, CIGA, CIGI, CISA - Senior Inspector General
Shawn Phillips, CIGA, CIGI, CECFE - Inspector General I

REPORT NO. 2021-01
JANUARY 20, 2021



Ken Burke, CPA

CLERK OF THE CIRCUIT COURT AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

Clerk of the County Court
Recorder of Deeds
Clerk and Accountant of the Board of County Commissioners
Custodian of County Funds
County Auditor

Division of Inspector General

510 Bay Avenue
Clearwater, FL 33756
Telephone: (727) 464-8371
Fax: (727) 464-8386
Fraud Hotline: (727) 45FRAUD (453-7283)
Clerk's website: www.mypinellasclerk.org

January 20, 2021

Teresa Del Rio, Executive Director, Court & Operational Services Division
Connie Daniels, Director, Court & Operational Services Division

We have conducted an audit of the Clerk's Office Driver License Transcript Data Exchange per management request.

An Opportunity for Improvement is presented in this report.

We appreciate the cooperation shown by the staff of the Court & Operational Services Division and Business Technology Services during the course of this review.

Respectfully Submitted,

Melissa Dondero
Inspector General/Chief Audit Executive

cc: Ken Burke, CPA, Clerk of the Circuit Court and Comptroller
Deborah Mells, Chief Information Officer, Clerk's Technology
Jeff Rohrs, Chief Information Officer, Business Technology Services



An Accredited Office of
Inspector General

TABLE OF CONTENTS

INTRODUCTION	4
<i>Abbreviations</i>	4
<i>Executive Summary</i>	5
<i>Background</i>	6
SCOPE AND METHODOLOGY	10
OBJECTIVES AND OUTCOMES	11
OPPORTUNITIES FOR IMPROVEMENT	12
1. <i>A Former Employee Retained Access To A Business Technology Services File Transfer Protocol Server.</i>	12

INTRODUCTION

Abbreviations

BTS	Business Technology Services
Clerk's Office	Clerk of the Circuit Court and Comptroller
County	Pinellas County
DHSMV	Florida Department of Highway Safety and Motor Vehicles
DL	Driver License
DPPA	Driver's Privacy Protection Act
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
SFTP	Secure File Transfer Protocol

Executive Summary

At the request of Court & Operational Services management, we conducted an audit of the Clerk of the Circuit Court and Comptroller's (Clerk's Office) Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) for the batch driver license (DL) transcript data exchange via batch job \$DTR504. The MOU (contract number HSMV-0444-19) was fully executed by the DHSMV on March 19, 2019.

The objectives of our audit were to:

1. Ensure the compliance of the Clerk's Office with the data security requirements in the data exchange MOU and applicable data protection statutes, codes, and policies.
2. Ensure adequate policies and procedures were in place to protect personal data provided to the Clerk's Office by the DHSMV through the batch DL transcript process.
3. Ensure adequate security over the access of the Clerk's Office and Business Technology Services (BTS) to DHSMV data through the batch DL transcript process.
4. Ensure adequate security over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process.

Except as noted in the report, the internal controls governing the use and dissemination of personal data obtained from the DL transcript data exchange have been evaluated in light of the requirements of the DHSMV MOU and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. This includes policies and procedures for personnel to follow and data security policies and procedures in place to protect personal data. The data security policies and procedures have been reviewed by a Risk Management IT Security Professional and found to be acceptable to protect personal data.

Our review revealed the Clerk's Office used the DHSMV's DL transcript data exchange solely for court purposes to make DL transcripts available during court proceedings. Although we determined a former Business Technology Services (BTS) employee retained access to a BTS server used in the DL transcript data exchange, BTS staff created a service request to remove the user's access upon our identification and notification. Therefore, this issue has been remediated to eliminate the risk of recurrence.

Background

The Pinellas County (County) Clerk of the Circuit Court & Comptroller (Clerk's Office) is responsible for the following:

- Maintaining custody of court records
- Maintaining custody of all related pleadings filed
- Securing evidence entered in court
- Ensuring the integrity of court files is protected
- Collecting and disbursing court fines and assessments and court-ordered child support
- Summoning prospective jurors

The Court & Operational Services Division is under the direction of the Clerk's Office. Within the division are the Criminal Court Records and Criminal Court Customer Service Departments.

The Criminal Court Records Department is responsible for filing, processing, and maintaining the following:

- Felony, misdemeanor, and other types of charges
- Juvenile dependency and delinquency
- Traffic and ordinance violations
- Non-criminal payable infractions

The main function of the Criminal Court Customer Service Department is to provide case assistance to the following entities:

- Public
- State Attorney's Office
- Public Defender's Office
- Salvation Army probation officers
- Department of Corrections probation officers
- Private attorneys for misdemeanor, traffic, felony, juvenile, domestic violence, payment plans, and Public Defender appointments

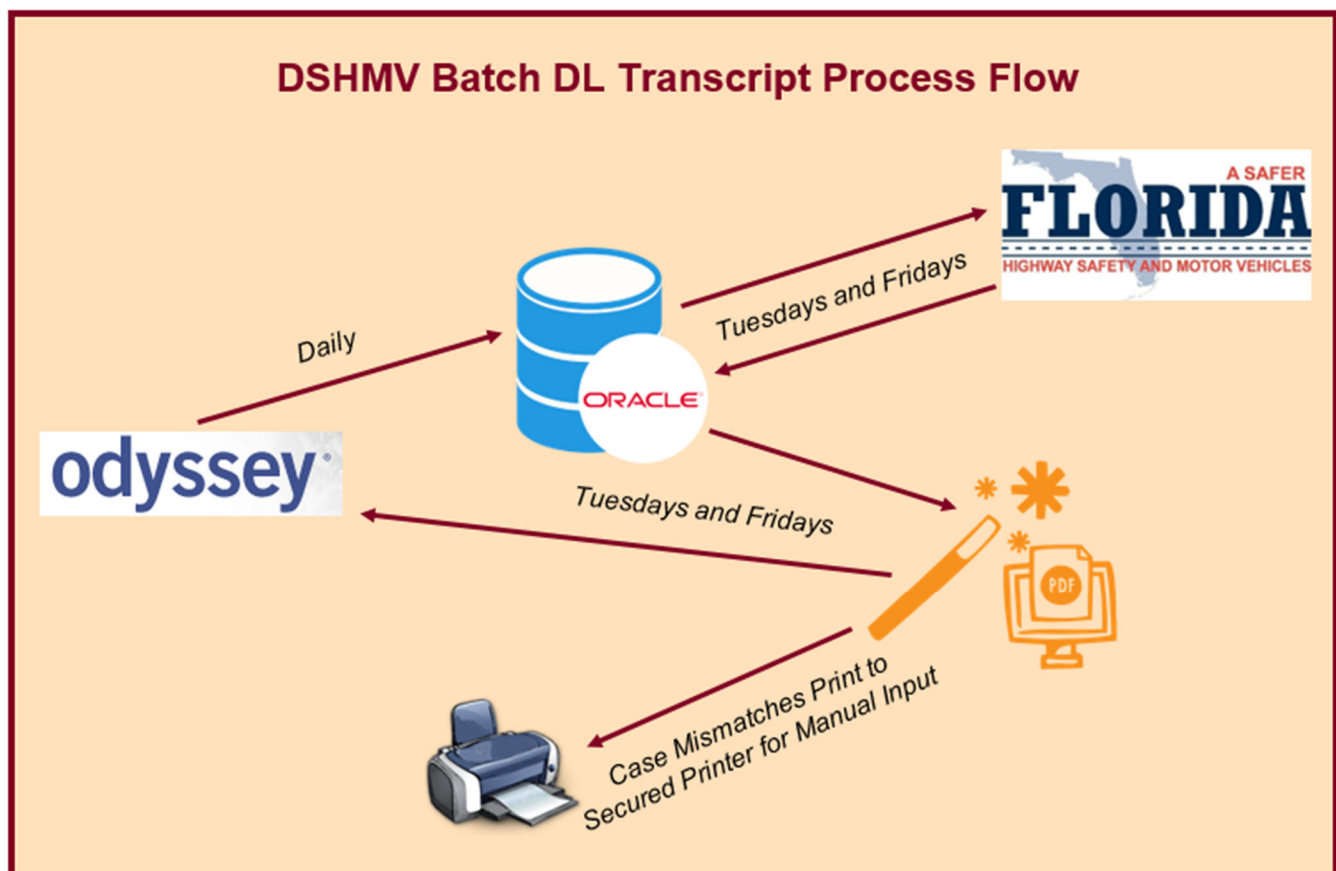
Misdemeanors and most criminal traffic cases are handled in County court. When traffic citation defendants take their cases to court, presiding judges need access to their driver license (DL) transcripts to assist in making judgments. The Clerk's Office has a data exchange memorandum of understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) to support court functions. The Court & Operational Services Division, in coordination with Clerk's Technology and Business Technology Services (BTS), facilitated a data exchange with the DHSMV in order to obtain DL transcripts. The data exchange leverages an in-house application to retrieve the necessary DL transcript data from the DHSMV, format the data, and upload it to the court case management system.

The automated DHSMV DL transcript process performs the following:


- Accesses the Odyssey court case management system daily to obtain a list of defendants scheduled to appear in court the following week
- Formats and sends a request to the DHSMV for the defendants' associated driver records twice weekly via secure file transfer protocol (SFTP)
- Retrieves the requested driver record data from the DHSMV via SFTP twice weekly
- Compiles each defendant's Odyssey case information and driver record into a single record
- Creates a DL transcript document for each defendant
- Accesses Odyssey and links the DL transcript document to the appropriate case event on the citation

The only deviation from the DL transcript process involves mismatched records that do not link to the Odyssey case automatically. In these instances, the mismatched DL transcripts print to a printer secured from public access. Staff performs research to identify the appropriate case for the mismatched DL transcript, scans the transcript, and manually attaches the transcript to the associated Odyssey case. During the audit, management implemented a process to ensure the printed transcripts were shredded after entry in Odyssey.

Following is an illustration of the DL transcript data exchange process:



Memorandum of Understanding

	Florida Department of Highway Safety and Motor Vehicles				
	Contract / Agreement Review				
DHSMV Contract No.:	HSMV-0444-19	Division:	Motorist Services	Date:	3/8/2019
Contractor Name:	Pinellas County Clerk of the Circuit Court and Comptroller				

The DHSMV provides services by partnering with County tax collectors and local, state, and federal law enforcement agencies to promote a safe driving environment. The department coordinates with its partners to issue driver licenses and identification cards, facilitate motor vehicle transactions, and provide services related to consumer protection and public safety. The DHSMV is composed of the following four divisions overseen by the Office of the Executive Director:

- Florida Highway Patrol
- Motorist Services
- Administrative Services
- Information Systems Administration

In carrying out its statutorily mandated duties and responsibilities, the DHSMV collects and maintains personal information that identifies individuals. Therefore, the DHSMV is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (DPPA), Sections 119.0712(2) and 501.171, Florida Statutes, and other statutory provisions.

The DHSMV Motorist Services Division has a data exchange MOU with the Clerk's Office signed by the Clerk's Office on February 13, 2019, and fully executed by the DHSMV on March 19, 2019. The agreement (contract number HSMV-0444-19) has a term of three years.

The DHSMV data exchange MOU provides the Clerk's Office access to three-year and seven-year batch DL transcripts to be used for court functions. The FTP batch job is \$DTR504.

As part of the agreement with the DHSMV, the Clerk's Office must secure all data associated with the data exchange. Section III., Legal Authority, of the MOU states the following:

"Under this MOU, the [Clerk's Office] will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the [Clerk's Office] agrees to maintain the confidential and exempt status of any and all information provided by the [DHSMV] pursuant to this MOU and to ensure that any Third Party End Users accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law."

Section VI., Compliance and Control Measures, Subsection A. of the MOU states the following pertaining to the required internal control and data security audit:

"Internal Control and Data Security Audit – This MOU is contingent upon the [Clerk's Office] having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The [Clerk's Office] must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a request from the [DHSMV]. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence."

The internal control and data security audit was originally due on March 19, 2020, which was the one-year anniversary of the MOU execution date. The Clerk's Office requested and was granted an extension until January 24, 2021.

SCOPE AND METHODOLOGY

We have conducted an audit of the Clerk's Office DL Transcript Data Exchange.

The scope of the audit covered the data exchange MOU between the Clerk's Office and the DHSMV to obtain batch DL transcripts. Section VI. A. of the MOU requires the completion of an internal control and data security audit on or before the first anniversary of the execution date of the MOU. Based on this MOU requirement and the applicable data protection laws referenced within the MOU, our audit scope was to assess the internal controls governing the use and dissemination of personal data obtained through the batch DL transcript process.

We ensured the internal controls in place were sufficient to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. In addition, we ensured that all deficiencies and issues found during the audit were corrected and measures enacted to prevent recurrence.

The audit period was March 19, 2019, through December 31, 2020. However, we did not limit the review of transactions and processes by the audit period and scope.

During the audit period we performed the following:

- Reviewed the data exchange MOU and referenced data protection statutes, codes, and policies.
- Reviewed BTS and Clerk's Office policies and procedures governing the protection of personal data.
- Reviewed flow diagrams, reviewed the program design, and conducted meetings with BTS and Clerk's Office staff to identify the path of DHSMV DL transcript data through County systems and all associated entry, exit, and storage points.
- Reviewed the controls in place to secure the machines and servers housing and executing the DL transcript program.
- Reviewed the controls in place to secure the DL transcript data transmissions between the DHSMV and the Clerk's Office.
- Reviewed the controls in place to secure DHSMV DL transcript data stored by BTS and the Clerk's Office.
- Reviewed the process to access the DHSMV SFTP service to download DL transcript data and ensured it was adequately controlled.
- Reviewed the physical security controls at BTS and the Clerk's Office to restrict access to computing equipment that housed the DL transcript application and DHSMV data.
- Conducted meetings with Court & Operational Services staff to understand how it distributed, used, modified, and disclosed, if applicable, DHSMV DL transcript data.

OBJECTIVES AND OUTCOMES

The objectives of the audit were to:

1. Ensure the compliance of the Clerk's Office with the data security requirements in the data exchange MOU and applicable data protection statutes, codes, and policies.
2. Ensure adequate policies and procedures were in place to protect personal data provided to the Clerk's Office by the DHSMV through the batch DL transcript process.
3. Ensure adequate security over the access of the Clerk's Office and BTS to DHSMV data through the batch DL transcript process.
4. Ensure adequate security over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process.

As a result of the audit, we determined:

1. The Clerk's Office was in compliance with the data security requirements in the data exchange MOU and referenced data protection statutes, codes, and policies.
2. The Clerk's Office and BTS had adequate policies and procedures in place to protect personal data provided by the DHSMV through the batch DL transcript process.
3. Overall, the security controls were adequate to restrict access to DHSMV data obtained through the batch DL transcript process. We noted an instance where a former BTS employee maintained access to the FTP server used in the batch DL transcript process. However, BTS immediately remediated the issue upon identification and notification.
4. There were adequate security controls in place over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process. Access to DHSMV data was controlled, and the data was used solely for court functions.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the *Principles and Standards for Offices of Inspector General*, and accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances.

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures, and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. A Former Employee Retained Access To A Business Technology Services File Transfer Protocol Server.

During our review of users with access to the FTP server used to exchange driver information with the DHSMV, we determined a former BTS employee had access to the server through membership in a security group.

The former BTS employee was part of a reorganization that resulted in a transfer to the Office of Technology and Innovation on January 7, 2018. Therefore, user access to the FTP server was no longer necessary.

Upon our inquiry, BTS completed a service request to remove the user from the security group on the FTP server.

For security purposes, relevant user names and security groups are not listed in this report. However, they were provided separately to management for remediation.

According to National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, an organization is responsible for the following with regard to privileged user account management:

- “(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;*
- (b) Monitors privileged role assignments; and*
- (c) Takes... organization-defined actions when privileged role assignments are no longer appropriate.”*

In addition, regarding disabling or deactivating accounts:

- “Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated.”*

NIST provides the following notification responsibilities for an organization:

“Notifies account managers:

- 1. When accounts are no longer required;*
- 2. When users are terminated or transferred; and*
- 3. When individual information system usage or need-to-know changes”*

Therefore, the former BTS employee's access should have been disabled as soon as the job change occurred.

The lack of a sufficient account review and cleanup process allowed the unnecessary user account to retain access. The user transferred to another technical function in the County, which resulted in some discussion during the audit about whether server access was still required.

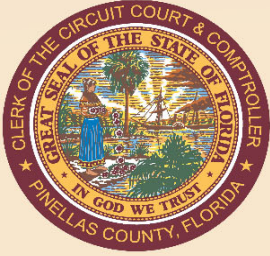
Allowing a user access to privileged system resources after leaving employment risks unauthorized access to view or modify critical data. In this case, the FTP server housed the driver information file obtained from the DHSMV.

We Recommend Management:

Work with BTS to ensure the identified employee's access to the FTP server used in the DL transcript process is disabled.

Management Response:

Management concurs and has verified the employee's access has been removed.



DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT
AND COMPTROLLER
PINELLAS COUNTY, FLORIDA

SERVICES PROVIDED

AUDIT SERVICES
INVESTIGATIONS
GUARDIANSHIP SERVICES
CONSULTING
TRAINING
COUNTY FRAUD HOTLINE
GUARDIANSHIP FRAUD HOTLINE
PCSO PREA HOTLINE



An Accredited Office of
Inspector General

Call: (727) 464-8371

Fax: (727) 464-8386

Fraud: (727) 45FRAUD
(727) 453-7283



Internet: www.mypinellasclerk.org

 www.twitter.com/pinellasig

 www.facebook.com/igpinellas



Write:

Division of Inspector General
510 Bay Avenue
Clearwater, FL 33756